Training Operating System v2.0

Welcome to Hacking School!

Please print this document, as it might be useful in case of any problems with booting or configuring the Training Operating System.

To start up the Training Operating System (TOS), please boot your computer from this disk. If you are already logged in MS Windows environment, you have to reboot the system. The Training Operating System does not require any additional HDD installation.

If you don't see the Hacking School welcome screen after rebooting the system, please make sure you had selected the proper boot device (CD/DVD drive) in the BIOS settings. To enter the BIOS, try to press (or hold) F2, F10 or DEL button during the boot. To change the boot order, please look for Boot, Advanced Bios Features or Boot Sequence menu. Set the CD/DVD drive as the first boot device.

This is a really simple procedure. If you're not able to manage, see FAQ for further details, check out our community Forum or use Google.

Minimal hardware requirements

- **CPU 500 MHz**
- **512 MB RAM**
- **CD/DVD ROM drive**
- **Graphics Card compatible with VESA**
- **BIOS with El Torito support**

Boot options

As soon as you start your computer from the CD, you will see the menu with available boot modes. Choose one, using arrow keys, and confirm the selection pressing Enter.

- **HackingSchool** - standard boot option, optimal for most configurations. If you experience any problems with graphics or you will see a black screen, try to boot in Vesa mode.

- **HackingSchool-Vesa** - tries to run the system in Vesa mode, that is, or at least should be, the standard for graphics card manufacturers. If you run TOS in default mode (see above) and booting ends in the console, the system probably is not able to identify your graphics card correctly. Using Vesa mode, you will be able to log into the X Window manager.

- **HackingSchool-FBDev** - runs TOS in framebuffer mode. Select this mode if both default and Vesa modes don't work.

- **HackingSchool-Safeboot** - safe mode, runs TOS without acpi, apic, scsi, pcmcia, and vesa support. For some hardware architectures, support for these standards causes problems (especially apic). If none of the above-described modes doesn't work on your computer, use this option.

- **HackingSchool-Console** - runs TOS in text mode and does not attempt to run the X Window System. The mode is useful for console and quick start fans.

- **HackingSchool-Copy2ram** - a system running in Copy2ram mode copies the contents of a CD into your computer's memory. To work in this mode, you need a minimum of 1 GB of RAM. When you copy a disk image to memory, CD / DVD drive will be released and you will be able to use it during the operation (eg to record something on the disc or to run the Live Training Videos directly from the DVD). Please note that copying the image to RAM may take a few minutes.

- **HackingSchool-MediaCheck** - checks the integrity of the media with the Training Operating System. If you run TOS in this mode, the system will verify that the CD was not damaged in some way. If you suspect that the disc may be damaged, first check its integrity. The successful verification of the media ends with a positive result.

- **Memtest** - runs Memtest86+ application, which is used to verify proper operation of RAM installed in your computer. If your computer becomes unstable, it may be caused by a failure of memory. Memtest helps you check it out.

Using the Training Operating System

Immediately after booting in graphical mode, you will see the welcome / login screen.

There are two basic user profiles in TOS. These are: root (administrator) and user (normal user without administrative privileges). On Unix systems it is assumed that the root is used to perform administrative and configuration tasks, while an ordinary user account is used for everyday use of the system. In other words, being logged in to an ordinary user account you will not be able to "harm" other users or the global system configuration, such as deleting important files. This is the theory... In practice, you'll use the root account quite often. The executing of certain applications requires system administrator privileges. In order to properly implement the training material and execute commands described in the Handbook, we recommend you to use the root account. Even if we make a mistake and accidentally delete important TOS configuration files or freeze the system (which is very likely to happen, for example when exploiting kernel modules) - do not worry. What you do is happening only in RAM of your computer. You can always restart your Training Operating System and everything returns to normal.

Remember, however, that this rule applies only to the main TOS file system. If, during operation, you mount one of the hard disk partitions in write mode, or connect a pendrive to USB port, the changes recorded in these partitions will be irreversible. By default, all external disks are mounted in /media directory. So remember not to execute any "dangerous" commands in that directory. You have been warned. If you are not using the resources of the hard drive and you don't need writing privileges, you can remount these partitions in read-only mode, minimizing the risk of removing important data. To remount selected partition in a read-only mode, use the command: *mount -o remount,ro /dev/hdxy*, where x is the drive letter, and y is the partition number. See the FAQ section to read a detailed description of this operation.

Log in as follows:

- **user: root, password: root**
- **user: user, password: user**

If you'd like to change the password of a selected user, use *passwd* command.

Some of the lessons present methods of increasing the privileges of a regular user. While reading the Handbook and watching the Live Training Video content you will notice that the hacker is working on several terminals, and on each of these terminals he is logged in as different user. If you are logged in on ordinary user account (user) and you want to change your privileges (become root), run the terminal and use *su* command. In this way, after entering the correct root password, you can work simultaneously as a normal user and administrator. You will not have to log out. It is very convenient, right?

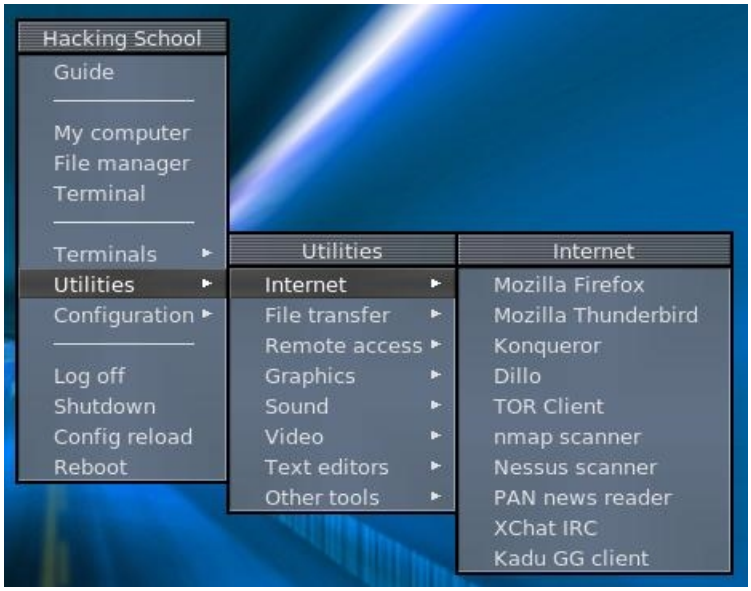
Working in X Window System

The default window manager in TOS is Fluxbox. Due to low hardware requirements and great configuration capabilities, Live Training material has been registered using this windows manager.

Fluxbox is very intuitive. Normally there are four virtual desktops on which you can run you applications. Please get familiar with available keyboard shortcuts - it'll help you navigate the system.

- **Alt + F1 - jump to 1st desktop**
- **Alt + F2 - jump to 2nd desktop**
- **Alt + F3 - jump to 3rd desktop**
- **Alt + F4 - jump to 4th desktop**
- **Alt + f - run Firefox browser**
- **Alt + k - run the konsole terminal**
- **Alt + y - run the yakuake terminal**
- **Alt + a - run the aterm terminal**
- **Alt + Tab - jump to the next window**
- **Ctrl + Alt + Fn - jump to the n-th text console**
- **Alt + F7 - get back to the window manager**

The main menu contains the available applications that run in graphical mode and is available by pressing the right mouse button on any point of the screen. Here's a screenshot.

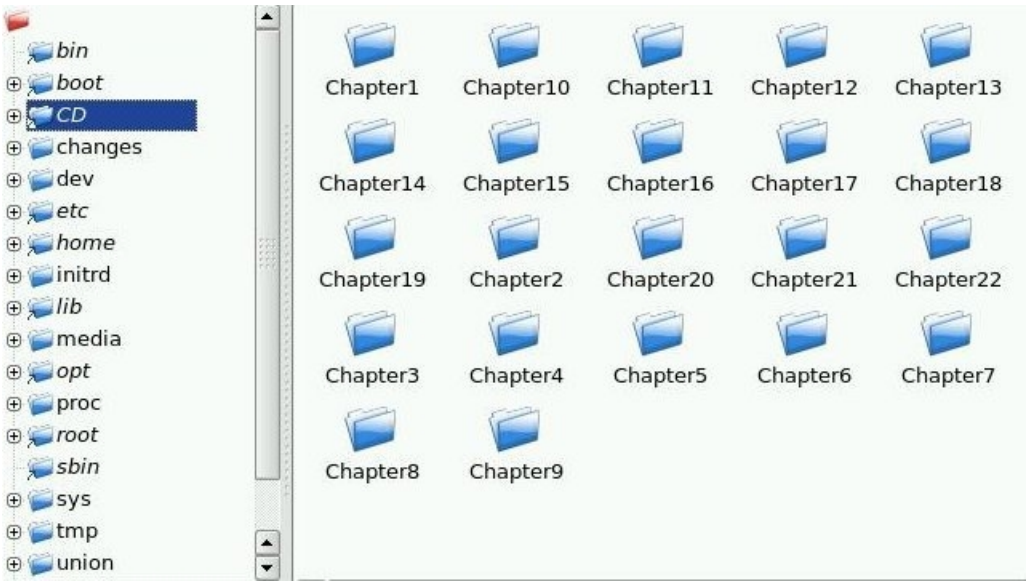


How to perform exercises described in the Handbook

All the source codes and the software that have been described in the Handbook, you will find in /CD directory in Training Operating System. You can get there using My Computer desktop shortcut or MC file manager. For your convenience the /CD directory contains chapter-oriented structure. If you, for instance, are working with the 5th chapter, you should enter the /CD/Chapter5 directory.

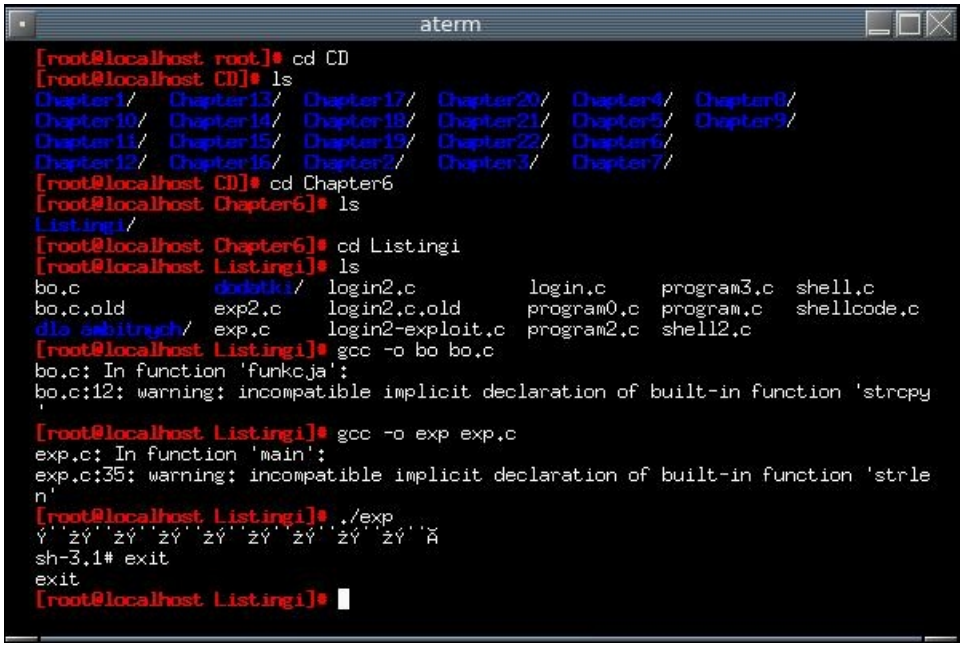
In each chapter folder you will find Listings and Software subfolders. Listings contains the source code shown in the Handbook. In Software subfolder you'll find all the software, ready for manual configuration and installation. Note that TOS already contains precompiled binaries of all applications you need. Though, if you use other Linux distribution, these packages might be useful.

Below you can find a sample screenshot of /CD directory:



Almost every Hacking School module begins with running a terminal. A real hacker should manage without a fancy graphical environment and mouse as well. In TOS you can find several great terminal emulators. Choose the one you like the most. The default terminal in TOS is *konsole*. In Live Training Videos we often used *aterm* terminal, but you can use *yakuake* or *xterm* as well.

Below you can find an example exercise from the 6th Hacking School module. Here's the screenshot.



Additional information

Remember! In order to minimize the risk of accidental data loss by an inexperienced user, we advise you to unmount all unused hard disk partitions or remount them to read-only mode as soon as the Training Operating System boots. Please see the FAQ for further details.

Frequently Asked Questions... and answers

1. **How to remount a partition to read-only mode?**
   There are several solutions available.

A) If you are familiar with the console and you know exactly which partitions have been already mounted, you can simply use the command: *mount -o remount,ro /dev/hdXY*, where X stands for the disk letter and Y stands for the partition number. If you have SATA hard disk, it will be probably available under /dev/sdXY path. The same principal applies to USB removable devices.

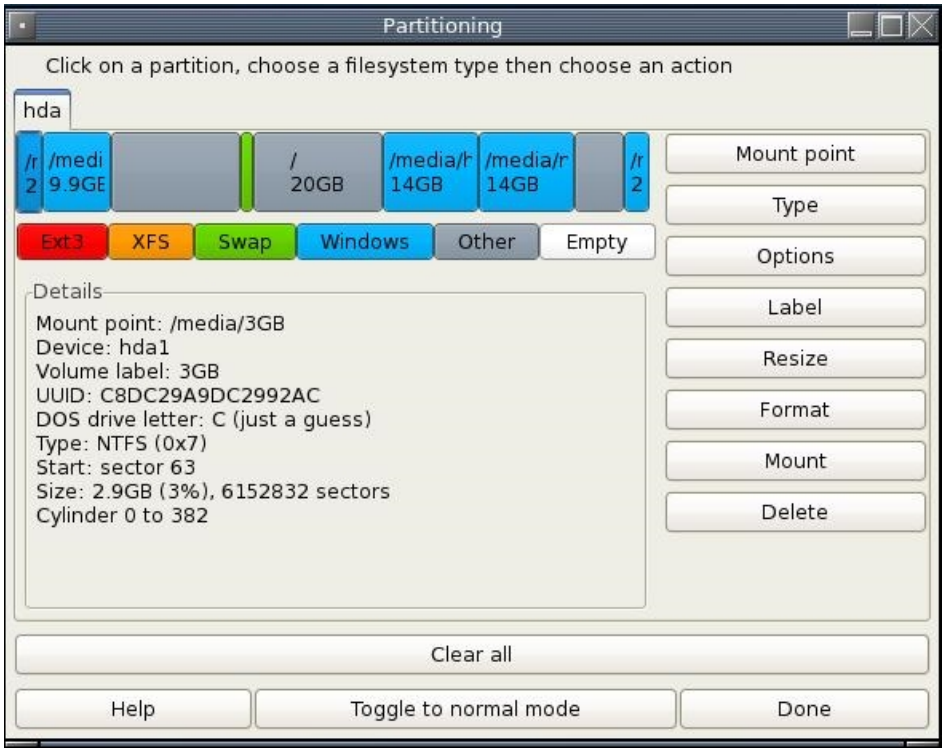
If you want to check out which partitions are mounted, use *mount* command. If you notice something like: */dev/hda2 on /mnt/e type fuseblk (rw,allow_other,blksize=4096)*, it means that the second partition (number 2) of the first hard disk (letter a) is mounted in the /mnt/e directory. Fuse was used, so we can suppose the partition use ntfs file system (fuse is used by ntfs-3g package to mount ntfs). Rw parameter means that the partition is mounted in write mode. To remount it to read-only mode, you can type: *mount -o remount,ro /dev/hda2*. Simple, isn't it?

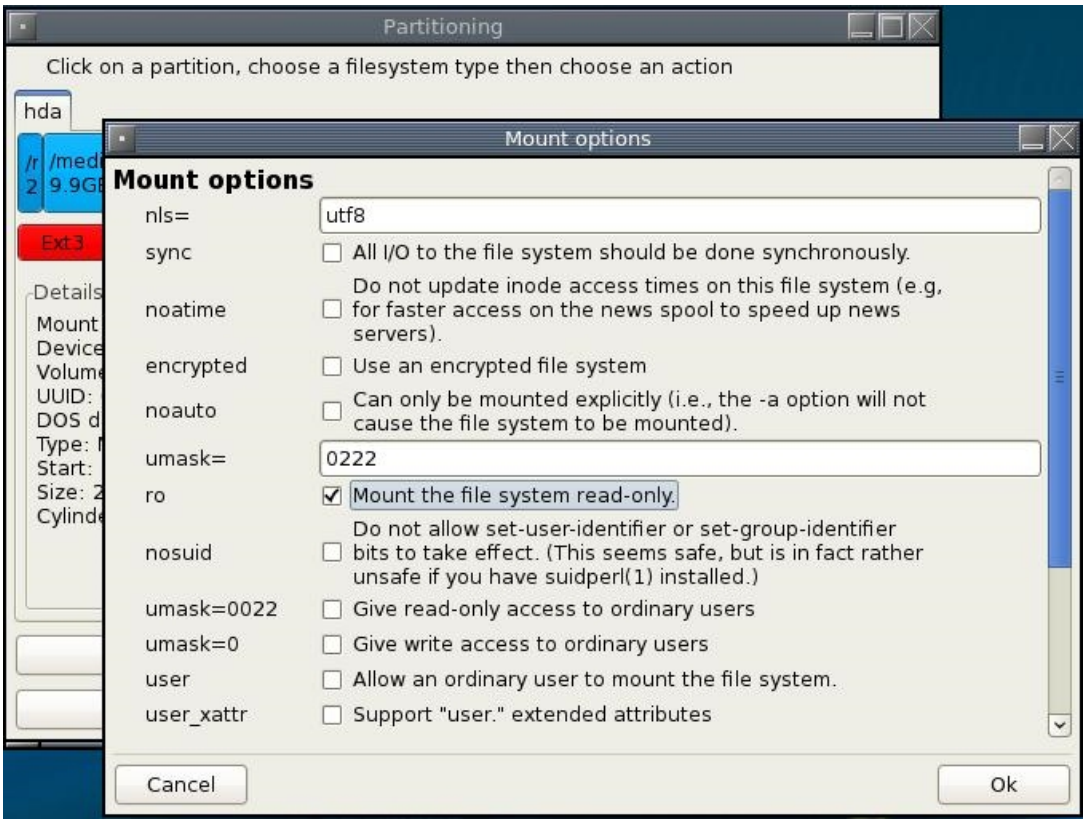
If you get something like *Remounting is not supported at present. You have to umount volume and then mount it once again.*, try to unmount the partition with *umount /dev/hda2* and remount it again with *ro* parameter, typing *mount -o ro /dev/hda2 /mnt/e*.

If there are no mounted partitions, you can list the partition table with: *fdisk -l /dev/hdX*, in this case we should run: *fdisk -l /dev/hda*.

B) The other solution is based on disk and partition manager - diskdrake. Choose the application from the *Configuration* menu or type *diskdrake* in a terminal. Click the button *Toggle to expert mode* on the bottom. Choose the partition and click *Mount point* to define the mount point (ie. /media/c). Confirm settings by clicking OK and get to the *Options* tab. Use mouse to select *ro - Mount the file system read-only* and click OK. You can now apply your settings clicking *Mount* and close the application (*Done*).

Here are the screenshots:





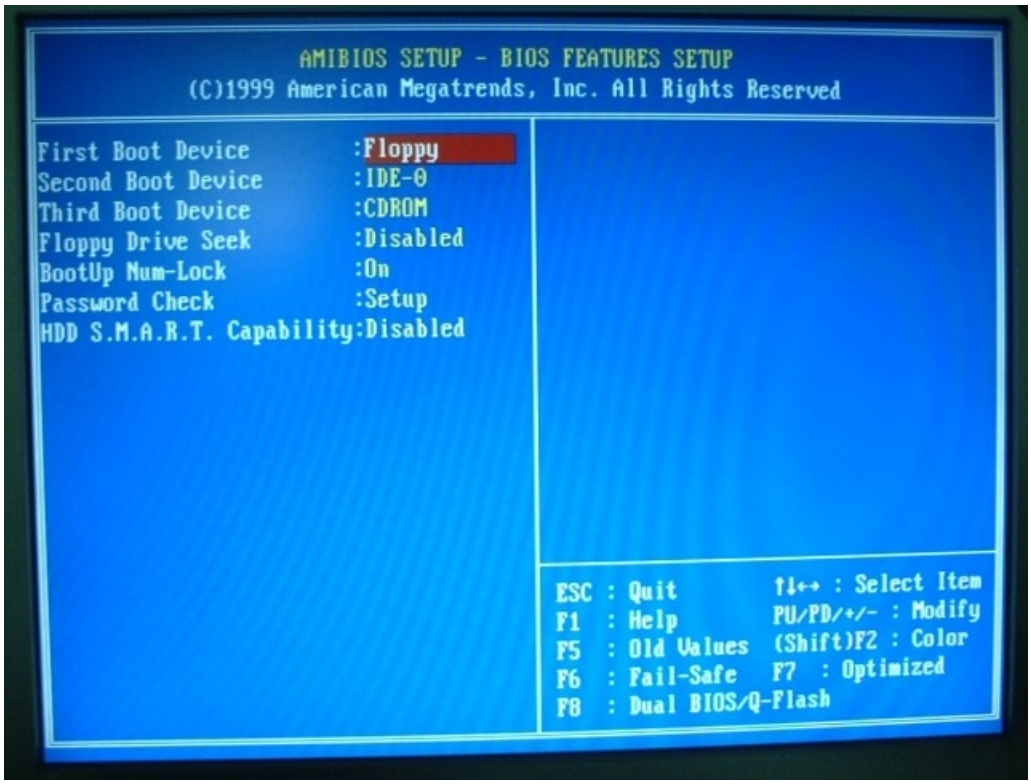
2. **After starting TOS I cannot connect to the Internet. What should I do?**
   Training Operating System is configured to automatically recognize your network devices. If your Ethernet network supports DHCP protocol, the eth0 interface should be configured during the startup. If you experienced any problems, run the *Network configurator* from the *Configuration* menu.

   If you use wireless network, proceed analogically, choosing the *Wireless* option in the application. If you can't find you network on the list, go back (*Previous* button) and try again - it'll force the application to re-scan. If your network is hidden, you can manually modify the settings and enter your SSID.

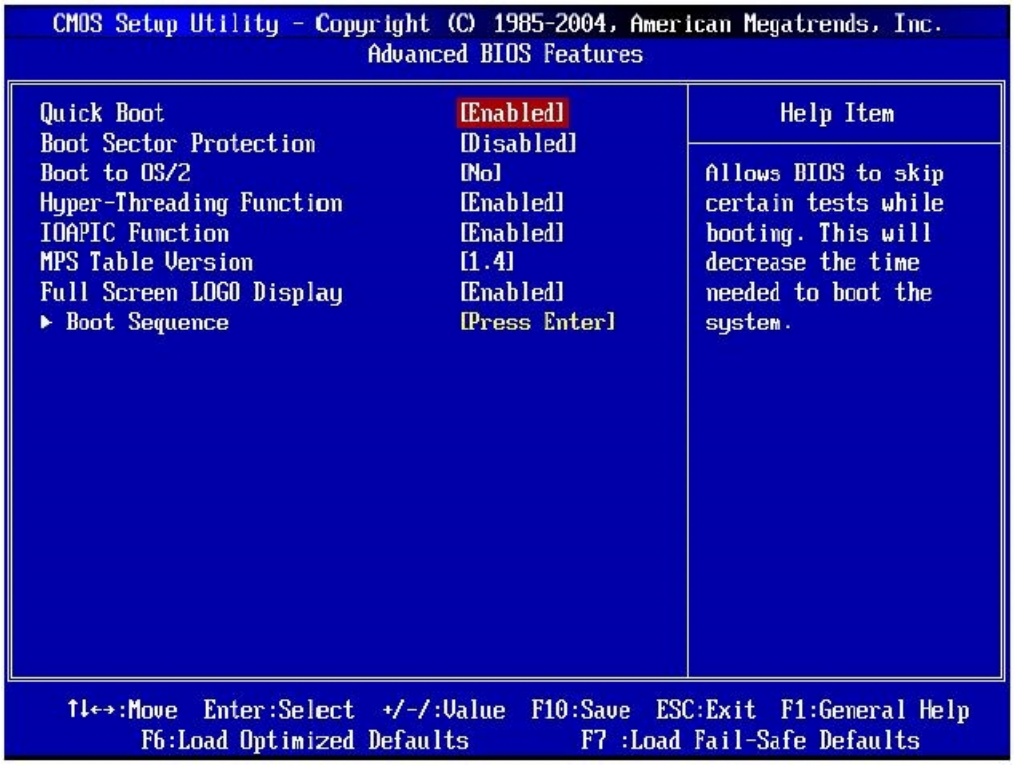
3. **I put the disc into the drive, reboot the computer, but the system does not start.**
   If you don't see the Hacking School logo after inserting the CD and rebooting the system, you must change the startup settings of your computer. To enter the BIOS, try to press (or hold) F2, F10 or DEL button during the boot. To change the boot order, please look for Boot, Advanced Bios Features or Boot Sequence menu. Set the CD/DVD drive as the first boot device. Change the settings in such a way that the CD / DVD drive is located on the top of the boot list. There are many different BIOS versions on the market and the configuration described above may be slight different in your particular case.

   Below you'll find screenshots of several popular BIOSes and places where you should make the appropriate changes.

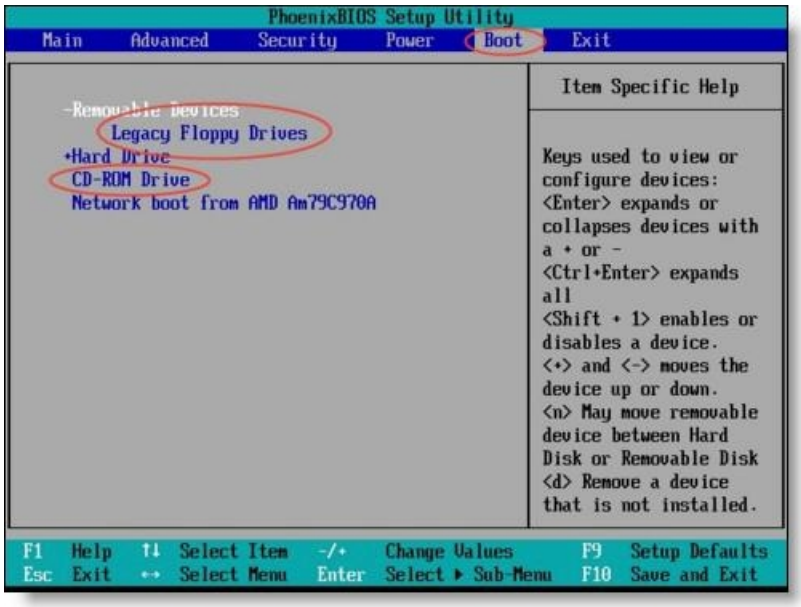
   AMIBIOS - change First Boot Device to CDROM and press Esc to save your changes.



AMIBIOS - Please select the Boot Sequence in the Advanced BIOS Features section.



Phoenix BIOS - enter the Boot tab, select the CD-ROM drive and move it to the top of the list, using the + and - keys.



4. **I tried all the available boot modes to run the TOS, but none of them works.**
   If you keep getting error messages related to access to your CD / DVD or livecd.sqfs file, please check the integrity of the media. After inserting the CD into the drive, select *HackingSchool-MediaCheck*. If the disc does not pass the verification, try to record it again.

   If the verification process ends successfully (*PASSED*), try to run the system using *HackingSchool-Safemode*. If that does not help, try to adjust the startup parameters. When you see the boot menu, press ESC and confirm your choice and go to the command line. Enter *school 3 livecd=livecd initrd=initrd.gz root=/dev/rd/3 acpi=off noapic nolapic noscsi nopcmcia vga=normal nosplash* and press Enter. It will run TOS in safe, text mode. You can also add other boot parameters, or remove them, according to your preferences.

   If the problem persists, you can run TOS in a virtual machine environment.

5. **Can I run TOS from a VirtualBox or VMWare virtual machine?**
   Yes, Training Operating System has been adjusted to work in VM environment. It contains kernel modules increasing the system performance in VirtualBox. To run TOS in MS Windows, download VirtualBox (it's free, you can get it here), use (or create) an ISO image of the CD and simply run the system. Of course you can rund the system directly from the TOS CD, but you will drasticly improve the speed and performance by creating the ISO image. To create the image, you can use free ImgBurn application. If you use Linux, you can accomplish the same with the command: *dd if=/dev/cdrom of=/media/your_disk/tos-image.iso*.

6. **I ran the TOS, but cannot log in. The system says that I give a wrong password.**
   To log into the administrator account, enter the username root and password root. User's password is user. After logging in you can change the password for selected user with *passwd* command.

7. **I have 512 MB of RAM. I noticed that sometimes the system does not respond.**
   512 MB of RAM is minimal amount the system needs to operate properly. The TOS, however, may operate very slowly when running multiple programs simultaneously. Upon exhaustion of the temporary memory, the system must perform many operations to read from the CD / DVD drive, which has significant effects on the performance. If your system is running slowly or mouse locks up from time to time, try to free some memory by closing unnecessary applications. To see the current memory usage, use the *top* command.

   As soon as the TOS boots, the Apache HTTP server and the MySQL database engine start. If you do not perform exercises from 7th or 20th module, you can close these services to free up some memory. To do this, type: */etc/init.d/httpd stop* and */etc/init.d/mysql stop*. That should give your system a breath.

8. **I ran the system in Vesa mode. After switching to the text mode (Crtl + Alt + F1), I see only a black screen.**

Yes, that may happen. Some of the graphical chipsets behave like this - it is a well known issue. Note that you can simply run another terminal in X Window environment or boot the TOS in HackingSchool-FBDev mode. That should resolve the problem.

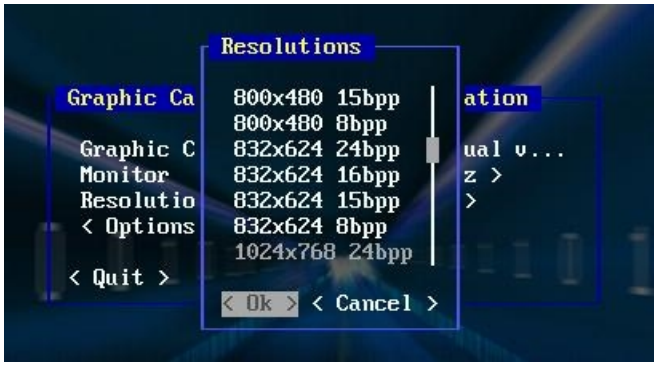
9. **How to boot TOS in FBDev mode using 1024x768 resolution?**
   By default the system boots in 800x600 resolution. The framebuffer runs in the resolution indicated by *vga* parameter. If you want to change the resolution, when you see the boot menu, press Esc to go to the command line and type: *school livecd=livecd initrd=initrd.gz root=/dev/rd/3 acpi=on vga=791 framebuffer*. You can also use F3 key to modify the default settings in graphical boot menu.

10. **I put the CD into the drive and chose the default boot mode (HackingSchool). The system doesn't boot at all - I see only a black screen.**
    Try to boot using Vesa, FBDev or Safemode.

11. **Running a window manager ends up with "Not optimum mode. Recommended mode 1440 x 900 60 Hz" error message.**
    Such a situation can occur if the system can not optimally configure the resolution of your monitor. The symptoms are typical for many LCD monitors from Samsung.

    To get rid of the problem, try to boot the TOS in HackingSchool-Vesa mode. In this situation, the system starts at the highest possible resolution offered by the native VESA driver. If you don't like the VESA mode limitations (low resolution and lack of the hardware acceleration), you can boot in HackingSchool-Console mode and then manually configure the resolution of X Window System.

    Login on root account (*login: root, password: root*), type *XFdrake* and press Enter. This brings up a window, where you can make the appropriate modifications. Use arrows to go to the *Resolution* tab, press Enter and select your preferred screen resolution (in this case it will be 1440 x 900). To accept your changes, press the Tab key to jump to the *OK* button and press Enter. If you want, you can also change other configuration settings. Finally, select *Quit* and confirm the configuration. Below you will find screenshots of these operations.



Type *kdm* and press Enter to run the window manager.

12. **Do I have to configure, compile and install the applications (./configure, make, make install) every time, as it is shown in the Handbook and Live Training Videos?**
    There is no such a need. Note that the Training Operating System contains all the applications described in the Handbook. The software is already installed and ready to use. The source code of these applications was added to let you follow the exercises in other Linux distribution. You can simply compile the application and use the exact same version that was described in

the Handbook. If you work with the TOS, you can skip these steps.

This, however, does not apply to source codes and examples contained in the *Listings* directory. These programs are designed to ensure that you read them carefully and understand their operation. That's why you should compile the sample programs and exploits by your own, in accordance with the instructions contained in the Handbook.

13. **I tried to compile the XYZ program, but I receive error messages. I'm using the ABC Linux distribution.**
    All source codes of the attached applications have been tested for proper compilation in Training Operating System environment. If you are using another Linux distribution, you must make sure your system contains all the required libraries. The Hacking School Support Team will not assist in this type of problems because there is an infinite number of possible configurations. If you can not deal with a problem, use Google, check out our community forum, or use the Training Operating System - it contains all the necessary tools in precompiled binary form. It is ready to use.

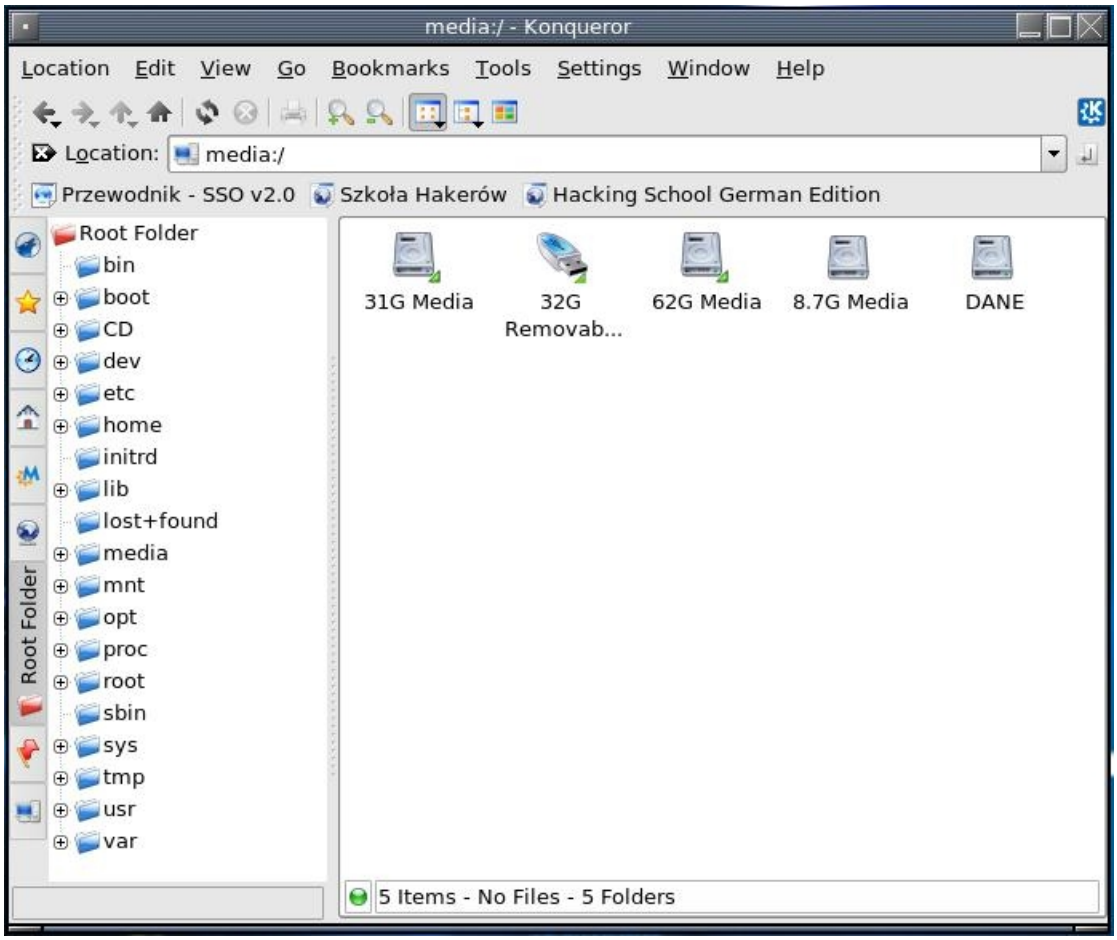
14. **In Live Training Videos the hacker performs *whoami* and *su* commands. What does it mean?**
    Live Training Videos were made using a regular user account (*user*). In order to perform certain configuration operations that require root privileges, the hacker issued the *su* command (su stands for SuperUser). The *whoami* command prints the name of your current user profile.

    If you have logged on root account, you don't need to use *su* command. If you want, you can issue the command *su user* to switch to a regular user.

15. **I don't understand what the XYZ command does. What should I do?**
    If you would like to learn more about some shell commands or application installed on your system, you can use *man program_name*. It will open the system manual with a program description.

16. **How can I get to my partitions and USB drive without having to mount them manually?**
    If you don't like the console and manually mounting seems difficult to you, click on *Disks and partitions* icon on your desktop. It will open the *konqueror* application, that should auto-detect all the available partitions. If you don't see your USB drive, try to use the *Refresh* button.

    Here are sample screenshots:



17. **The Fluxbox window manager is ugly. Do I have to use it?**
    No, you don't. You can choose *KDE* from *Sessions* menu. Make your changes on the *kdm* welcome screen. Please note that Fluxbox is very lightweight, super-fast, configurable and functional environment. It does not burden your system with a whole bunch of unnecessary processes.

18. **I have a wireless network adapter based on rt61pci chipset (ie. Pentagram horNET WiFi PCI). The installation in *Network configurator* ends up with errors or freezes my computer. What should I do?**
    Try to use *ndiswrapper* option and upload your windows drivers. Enter the */lib/firmware /ndiswrapper-rt61-rt25xx-rt26xx* directory and select *rt61.inf* file. This time your card will be configured correctly.

19. **I have a XYZ wireless network card. The system does not recognize it and I can't connect to my network.**
    Look for the CD with drivers or locate the files on your main Windows partition. Use *ndiswrapper* in the *Network configurator* and upload the driver (selecting appropriate *.inf* file). Your card should be configured using Windows driver.

20. **In the Xth chapter of the Handbook has been written that I should pass the 0xbffff3c6 argument to the application. It doesn't work in my case.**
    This is normal. During exploitation of sample programs, you will often face such situations. Addresses in the program memory change and it depends on many factors. In the Handbook you will find the detailed description of every technique and it will allow you to adjust these addresses manually to your specific situation. You will get to know how to check the address of the injected shellcode - take advantage of it. Please note that you cannot treat these addresses as constants. Your goal is to gain universal knowledge and to completely understand the essence. If you understand the theory and you can apply it in practice, you won't have any problems with implementation of the newly acquired skills in different conditions.

21. **I'd like to save my network configuration and downloaded files. Can I save changes in TOS on the hard disk?**

In default configuration the TOS saves changes in RAM. After restarting, memory is cleared and your modifications are no longer available. If you would like to save your changes on hard disk, use *changes_dev* and *changes_file* boot parameters.

Parameter *changes_dev* means a device which will store your changes, while *changes_file* parameter is the name of the file. Let's look at an example. Start the Training Operating System. When the startup menu appears press *Esc* and go to the command line. Type: *school livecd=livecd initrd=initrd.gz root=/dev/rd/3 vga=788 splash=silent keyb=en lang=en acpi=on changes_dev=/dev/hda1 changes_file=/changes* and press Enter. TOS will run in graphical mode (*vga=788* means 800x600 resolution), with english keyboard and language settings (*keyb=en*, *lang-en*) and ACPI support (*acpi=on*). Parameter *livecd=livecd* means that the system will look for the main boot file called *livecd.sqfs*. It will also load the initial ramdisk with drivers and preboot scripts, located in the *initrd.gz* file and activate the ramdisk (*root=/dev/rd/3*).

During boot the file */dev/hda1/changes* will be mounted as so-called loop device and it will store all your changes.

Attention. The *changes* file must exist and contain an ext2/ext3 filesystem. Changes can be saved on ext2/3, FAT16 or FAT32 partitions. NTFS partitions are not supported during the initialization phase. If you have not prepared the *changes* file yet, you can do this as follows:

1. **Mount selected partition with *mount* command, for example: *mount /dev/hda1 /media/disk***
2. **Create an empty file and name it as *changes*. We will assign 200MB for our purposes: *dd if=/dev/zero of=/media/disk/changes bs=1M count=200***
3. **Format the *changes* file using ext2 filesystem: *mkfs.ext2 /media/disk/changes*. Press *y* to confirm.**

In this way you created a 200MB *changes* file, which can be used during boot. Note that the *changes* file will contain only the changes you make inside /union directory. Most of the system directories are mapped in /union. Therefore, if you save something in /etc, /root or /home/user director, your changes will be immediately saved to the file. Be sure to proceed with caution. A small typo can lead to permanent damage of your data.

22. **Is it possible to install the Training Operating System on the hard drive?**
    In order to install the Training Operating System on the hard drive, go to the *Configuration* menu, click on the *HDD Install* option and follow the wizard. Note that the installation process is intended for advanced Linux users only. The installation process interferes with the physical structure of the hard disk (for example when writing the master boot record), which in the hands of an inexperienced user may result in data loss. If you are a beginner and would like to speed up the Training Operating System, we encourage you to complete the installation in a Virtual Machine environment.

The Training Operating System is based on PCLinuxOS which derives from Mandriva Linux. PCLOS is a great project, developed by real Linux enthusiasts and very active community. If you would like to contribute and make a modest donation, click here.

Good luck!
Hacking School Support Team